Hoaxes en kettingmails

Inbox-terrorisme!

Nee, we hebben geen wit poeder in onze e-mailbox gevonden. Wel een aantal merkwaardige e-mails over superdestructieve virussen en over zieke kindjes: *hoaxes*. Wat doe je ermee? Waar komen alle varianten vandaan? Clickx Magazine ging op zoek naar waarheid en leugen in zo'n kettingmails, gewapend met de delete-toets van het toetsenbord.



Het leek wel onze geluksmaand: we konden de trotse eigenaar worden van een puppy uit een verlaten nest Golden Retrievers, van $ 1.000 ons persoonlijk overhandigd door onze vriend Bill Gates, en daarbovenop ook 8,3 miljoen dollar uit de kas van de Nigeriaanse Kamer van Koophandel. Als we geïnteresseerd waren in dat laatste aanbod, moesten we een e-mail sturen naar Prince Tunji Mohammed, om te zeggen dat we recht genoeg in onze schoenen stonden en dat we voor hem een rekening wilden openen in ons land. Daarop zou hij dan zo'n slordige 40 miljoen dollar kwijt kunnen. Tussendoor hebben we ook nog onze Hotmailbrievenbus en een kindje met een ingeklapte long gered, en hebben we onze volledige vriendenkring gered van een levensgevaarlijk virus, het zogenoemde Awereness-virus, dat de pc-gebruiker ertoe zou aanzetten om... te vroeg op de Verzendknop te drukken.

Ga en vermenigvuldig u!

Om onze wildste dromen werkelijkheid te doen worden of om te redden wat er te redden valt, hoefden we maar één ding te doen: de e-mail die ons toegezonden werd, doorsturen naar alle adressen uit ons adresboek. Als je het zo leest, klinkt het als waanzin. En toch bewijst zowat elke e-mailinbox elke week dat er nog steeds goedgelovige mensen zijn die zich laten vangen door zogenoemde e-mailhoaxes. Het Engelse woord hoax betekent letterlijk bedrog of grap. Een flauwe grappenmaker of soms ook echt iemand met foute bedoelingen, lanceerde 'ooit' een valse waarschuwing of een oproep en de internet-geruchtenmolen doet zijn werk. De 'hoax' verspreidt zich razendsnel. Zelfs als alleen de helft van de 'eerste generatie' ontvangers goedgelovig is en het bericht doorstuurt naar tien vrienden en kennissen, dan krijg je toch meteen een enorm sneeuwbaleffect. En vanaf dan ontstaan er ook licht gewijzigde versies, die soms jaren nadien weer opduiken: de kettingmail heeft zoveel levens dat je er een kat jaloers mee kan maken. Hoaxes lijken op het eerste gezicht een nest waarin de kat van daarnet ook haar eigen jongen niet meer zou herkennen. Als je je als e-mailgebruiker wil wapenen tegen die nepberichten en kettingbrieven, dan kan je maar beter de drie grote categorieën van hoaxes eens op een rijtje zetten. Zo heb je virushoaxes die je waarschuwen voor nepvirussen, de telhoaxes die op de een of andere manier de internetgebruikers willen tellen en tenslotte de oplicht-hoaxes.

De ingebeelde zieke

Wie hoaxes zegt, denkt in de eerste plaats aan massamails die waarschuwen voor ultra-gevaarlijke computervirussen die de harde schijf van je computer opblazen, je huis doen instorten of de vrouwentongen op je vensterbank vergiftigen. Volgens de website van een Amerikaans computerbeveiligingsbedrijf [http://hoaxbusters.ciac.org], was een van de eerste hoaxes zo'n waarschuwing voor een nepvirus: het 2400 baud modemvirus. Het bericht werd in oktober 1988 geschreven in naam van een software-ontwikkelaar, die zogezegd ontdekt had dat er zich in een 'snelle' 2400-baud modem een virus kon nestelen. In november van hetzelfde jaar kwam er een ludieke reactie van iemand met gezond boerenverstand:

```
Warning: There's a new virus
on the loose that's worse than
anything I've seen before! It
gets in through the power
line, riding on the powerline
60 Hz subcarrier. It works by
changing the serial port pin-
outs, and by reversing the di-
rection one's disks spin.
Over 300,000 systems have
been hit by it here in Mur-
phy, West Dakota alone! And
that's just in the last 12 mi-
nutes.
```

Met andere woorden: er was een virus gesignaleerd dat zich via het stopcontact een weg naar de computer baande. Let vooral op de locatie: Murphy! Het advies van de auteur was geen elektriciteit meer te gebruiken... Sindsdien is dit soort paniekerige paranoia van computergebruikers wereldwijd alleen maar toegenomen. Het Britse antivirusbedrijf Sophos houdt op haar website [www.sophos.co.uk/virusinfo/infofeed/more.html#hoax] een maandelijkse top 10 bij van de 'populairste' virushoaxes. En je kan ook gratis een top 5 van hoaxes op je eigen website publiceren. De updates gebeuren automatisch via Sophos. Zo stond in december 2002 bijvoorbeeld de JBDGMGR-hoax op kop, ook wel Teddy ge-

GRATIS?

Een hoax kan zich sneller verspreiden dan de besmettelijkste ziekte dankzij het monster 'tegelijk'. Het kost de ontvangers weinig moeite (en op het eerste gezicht al evenmin geld) om naar vele mensen tegelijk een e-mail te versturen. Die gebruiksvriendelijkheid van het internet kan de internetproviders wél duur te staan komen, want hun servers moeten alle boodschappen tijdig verwerkt krijgen. Stel dat iemand een hoax stuurt naar tien personen uit z'n adresboek. Hij vraagt in z'n bericht steevast om het e-mailtje naar minstens tien mensen uit je adresboek te sturen. Als alle tien ontvangers van de eerste generatie hun bericht forwarden naar tien anderen, dan zijn er al honderd nieuwe ontvangers in de tweede generatie. Dat aantal groeit exponentieel en in de zesde generatie heb je al 1.000.000 nieuwe bestemmelingen. De *mailservers* van providers kraken onder de druk van al die onnodige, paniekerige (en onjuiste) berichten. Oplossing is de snelheid van de servers te verhogen, en daarvoor zal jij als klant van een internetprovider dan uiteindelijk toch betalen. En er is nog een andere kost: je tijd om zo'n hoax te in te schatten! Is het waar, is het niet waar? Je twijfelt onvermijdelijk en voor je het weet ben je een minuut bezig met zo'n bericht. Als 1.000.000 mensen één betaalde minuut verliezen, loopt dat algauw in de miljoenen euro's aan extra werkingskosten. En dat zal je baas niet graag horen.

VAKTAAL

Hoax: Nepvirus. Een hoax is een waarschuwing in de vorm van een e-mailbericht voor nieuwe (al dan niet echte) virussen. Wie zo'n bericht ontvangt, wordt aangespoord om het door te sturen naar al zijn kennissen. Op die manier willen de bedenkers een massale e-mailstroom genereren in de hoop zo hetzelfde effect te bereiken als een worm-virus: het e-mailverkeer te vertragen en e-mailservers lam te leggen.

Mailserver: Een mailserver is een computer die de ontvangst en verzending van elektronische post verzorgt.

noemd. In de nep-virusmelding krijg je het advies om een uitvoerbaar bestand (jbdgmgr.exe) dat mogelijk op je harde schijf zit, te wissen, omdat boze mensen via dat bestandje en je internetverbinding je kredietkaartnummer en alle paswoorden zouden kunnen buitensmokkelen. Het bestandje blijkt bij nader inzien een onderdeel van je besturingssysteem, dat je nodig hebt om programma's in de programmeertaal Java, meer bepaald in Visual J++, te schrijven. De verwarring ontstond waarschijnlijk doordat jbdgmgr.exe een grijs beertje als icoontje heeft. En dat wekt uiteraard argwaan bij pientere maar niet-programmerende computerliefhebbers die iets gehoord hebben over het (échte) BugBear-virus dat zichzelf toen vrolijk rondstrooide. Een ander misverstand dat ooit de ronde deed was dat er een 'Bloodhound'-virus bestond. Bloodhound is echter geen virus, maar wel een boodschap die het antivirusprogramma van Symantec op het scherm toont als het denkt dat het een virus ontdekt heeft. Daarmee is meteen verteld dat nep-virusmeldingen vaak rondgestuurd worden door 'onwetende' computergebruikers. De makers van de hoaxes spelen daar trouwens op in door ingewikkelde en technische termen te gebruiken, zoals je al kon zien in het eerste modem-nepvirus. Maar ook mensen met kennis van zaken kunnen zich laten vangen: zo kreeg het nepvirus 'A Virtual Card for you' nationale zendtijd via Belga en de VRT-radio in september 2001. 'A Virtual Card for you' staat nu nog steeds in de top 10, en is volgens de kenners een echte klassieker. Het zou (alweer) het ergste virus ooit zijn, en erger nog, antivirusbedrijven McAfee en Norton, de hoop van de voltalige mensheid, hebben nog geen tegengif. Ter verdediging van de overijverige journalisten: in de tekst van het hoax-bericht zaten er een aantal erg aantrekkelijke 'krenten' verstopt: er wordt naar CNN verwezen, en er zou zelfs een werknemer van Microsoft zijn die het virus geopend heeft. Waarheid van fictie onderscheiden is niet echt simpel, en daarom kan je maar beter sowieso nooit, we herhalen, nooit, virusmeldingen doorsturen. Het is simpelweg niet jouw taak als gewone pc-gebruiker thuis of op het werk en vaak zorg je alleen maar voor platte paniek. Antivirusfirma's zullen de zaak wel uitklaren, al zijn sommige ook niet echt vies van een beetje virushysterie om hun producten beter te doen verkopen.

Position	Hoax	Percentage of reports
1	JDBGMGR	13.7%
2	Budweiser frogs screensaver	10.7%
3	A virtual card for you	7.2%
4	Bonsai kitten	7.0%
5	Meninas da Playboy	6.6%
6	Hotmail hoax	6.0%
7	WTC Survivor	5.7%
8	Elf Bowling	3.6%
9	Mobile phone hoax	2.9%
10	Frog in a blender/Fish in a bowl	2.8%
Others		33.8%

De top 10 van Sophos in december 2002: allemaal vermeende vieze beestjes.

Nog een andere virushoax uit de top 10 van december 2002, om het af te leren: de 'Budweiser frogs screensaver'. Budweiser is een Amerikaanse bierfirma die in 1997 een leuke kikker-screensaver op z'n website plaatste, naar aanleiding van een tv-spotje met kikkers. Het werd een soort hype en daar hoort uiteraard ook een hoax bij. De kikkers vermommen zich volgens de e-mailhoax als *Trojaanse paarden* die allerlei stoute dingen doen in je pc. Weet hoe dan ook dat je altijd op je hoede moet zijn voor 'uitvoerbare' bestanden, met

Hoe herken je een hoax?

Een hoax is bijna een literair genre, met een typische structuur. Stel jezelf de volgende vragen, begin alvast een frons op je voorhoofd, en hou je vinger boven de delete-toets.

1 Heeft je verdachte bericht een drieledige structuur?

Het begint met een hook: 'Dit is erg dringend mensen', 'lees dit', of zelfs: 'dit is geen hoax'. Daarna komt de 'threat': 'er is een supergevaarlijk virus en zelfs onze redders in nood McAfee en Symantec weten niet wat te doen.' Dan volgt de 'request': 'je moet het mailtje doorsturen naar al je vrienden' ('ook al heb je er niet veel,', staat er dan!). Eigenlijk is dat laatste de essentie van elke hoax. Als de tekst je vraagt het bericht door te sturen naar zoveel mogelijk mensen, wees dan op je hoede.

2 Staat het bericht vol techno-blabla?

Dat is taal die erg chic en technisch klinkt, maar bij nader toezien nergens op slaat. Deze vonden we best indrukwekkend: een nepvirus dat de processor van onze pc in een 'nth-complexity infinite binary loop' zou brengen. Wie er niks van kent, is onder de indruk, wie wel verondersteld is er iets van te kennen, durft niet te zeggen dat hij het in Keulen hoort donderen.

3 Komt het bericht rechtstreeks van een expert op het gebied van computerbeveiliging?

Of stuurt je schoonmoeder je dit bericht, dat ze op haar beurt via de buurvrouw kreeg, van wie de man een computerexpert is? Dat is verdacht, want een hoax zal altijd proberen een referentie naar een betrouwbare bron in te bouwen. Denk aan Bill Gates, Microsoft, CNN,… Antivirusbedrijven figureren als vanzelfsprekend vaak in virushoaxes. Een professor of een ingenieur werkt ook altijd.

4 Word je doorverwezen naar een betrouwbare webpagina?

Normaal bevatten échte virusmeldingen niet al te veel details. Je krijgt een samenvatting, en als je meer wil, surf je naar de site van een betrouwbare antivirusfirma. Let wel: sommige hoaxes gebruiken algemene links naar bijvoorbeeld [www.mcafee.com]. Een echt virusbericht zal een rechtstreekse link geven naar informatie over het virus.

5 Beginnen waarheid en leugen voor je ogen te dansen?

Kijk dan even na of je de naam van het (nep)virus kan terugvinden op een van deze gespecialiseerde anti-hoax sites:

[www.symantec.com/avcenter/hoax.html]
[http://vil.mcafee.com/hoax.asp]
[www.vmyths.com]
[www.f-secure.com/virus-info/hoax]
[http://hoaxbusters.ciac.org]



een .exe extensie. Daar hoef je verder geen persoonlijke waarschuwingen naar vriend en vijand voor te sturen.

Pas op je tellen!

Een andere favoriete bezigheid van makers van hoaxes, is tellen! Zo zijn er mails van Bill Gates himself in omloop. De tekst luidt:

```
Hello everybody,
My name is Bill Gates. I have
just written up an e-mail tra-
cing program that traces
everyone to whom this messa-
ge is forwarded to. I am ex-
perimenting with this and I
need your help. Forward this
to everyone you know and if
it reaches 1.000 people
everyone on the list will re-
ceive $1.000 at my expense.
Enjoy.

Your friend,
Bill Gates
```



Er leeft een hardnekkige mythe op het internet dat e-mails getraceerd en geteld kunnen worden als ze een ketting vormen. Er mag dan al iets bestaan als 'gelezen'-meldingen voor e-mail, maar het is absoluut onmogelijk om op dit moment een mailtje doorheen cyberspace te volgen, laat staan dat je duizend mailtjes op kan sporen. Als Bill Gates zich dan al persoonlijk zou bezighouden met het verzenden van mailtjes naar jan en klein pierke, natuurlijk... Er zijn ook allerlei varianten op dit bericht gekomen. Een ervan is waarschijnlijk echt lucratief: Bill Gates stuurde zogezegd een opvolgingsmail om ons de blijde boodschap te brengen dat de duizendste mail verstuurd was en dat het dus tijd werd om met het geld over de brug te komen. Je hoefde alleen maar je kredietkaartnummer en vervaldatum door te geven en het bedrag zou op je rekening gestort worden...
Het telsyndroom is ook ooit populair geweest bij GAP, een Amerikaanse kledinggigant. Er bestaat een hoax die je vraagt om mee te doen aan een nieuw systeem: voor elke persoon naar wie je het bericht forward, krijg je een onderbroek, voor elke persoon aan wie jouw contact een e-mail stuurt, krijg je een T-shirt met Hawaïprint, en voor gekken in de derde graad ligt er zelfs een heuse vissershoed klaar. En als je dat niet gelooft maken we je iets anders wijs... Bijvoorbeeld dat Microsoft Hotmail gaat afschaffen, of tenminste dat ze je e-mailbox gaan afsluiten omdat er de laatste tijd te veel ongebruikte e-mailboxen bijgekomen waren... Je kan je mailbox alleen redden als je de waarschuwingsmail naar minstens tien contactpersonen doorzendt.

Een hoax met telefoonnummer?

Een tijd geleden kregen we een hoax over een jongetje met een ingeklapte long. De ouders, Ria en Koos, konden de operaties niet meer betalen. Gelukkig had hun verzekeringsmaatschappij een deal gesloten met de provider 'Het Net': voor elke forward van het mailtje, krijgen de ouders 5 cent. Tot hiertoe: alle kenmerken van een onvervalste hoax. Alleen, er stond zowaar een naam, inclusief telefoonnummer in België en exact adres onder de mail. Nog straffer: de vrouw die tekende heette Ria... Zoals de mama van de (on)fortuinlijke zoon dus? Wij hebben haar gewoon opgebeld en we waren niet de eerste. Ria uit West-Vlaanderen had geen zoon met ingeklapte long, maar had de hoax-mail wel doorgestuurd, en per ongeluk was haar e-mailhandtekening onderaan de mail gesukkeld. Precies een jaar geleden, vertelde ze ons. Maar waarom stuurt ze zo'n dingen door? Simpel: uit medelijden: ze heeft zelf een dochter die niet kerngezond is en ze herkende de situatie. Bovendien had zij de mail van een collega gekregen en die vertrouwde ze blindelings. Ze dacht, even doorsturen, en dan ben ik er vanaf. Niks was minder waar, want ze kreeg het afgelopen jaar telefoontjes van over de hele wereld en zelfs enveloppes met geld, zo'n € 200. Ria wist ons te vertellen dat ze het geld altijd probeert terug te sturen, en als de milde schenker niet te vinden is, maakt ze het over aan een goed doel.

Mysterie

Sjeiks en consuls stralen altijd iets chics en mysterieus uit. Dat is de ideale cocktail voor een hoax. Het mystery-sfeertje wordt in dit geval niet opgewekt door de technische blabla, maar wel door het exotisme van de auteurs. Geef toe: wie voelt zich niet een beetje vereerd als hij een mail van de consul van Nigeria krijgt? Helaas heb je waarschijnlijk een ordinaire oplichter aan de haak, of zijn vrouw/weduwe. Via een ingewikkelde constructie met banken, erfenissen, en Kamers van Koophandel beland je voor je het weet in de misdaad. Misschien zijn mensen sneller op hun hoede als er écht geld mee gemoeid is? Hoe dan ook, e-mail is altijd een beetje reizen...

— Bart Goossens —

VAKTAAL

Trojaans paard: Een gemeen programma dat voor vervelende problemen kan zorgen. De gebruiker heeft dit niet door omdat een Trojaans paard heimelijk iets anders doet dan hetgeen de gebruiker verwacht. Ze zullen bijvoorbeeld je gebruikers-identiteit en wachtwoord stelen en doorzenden naar iemand anders.